**KİŞİSEL VERİ**

**SAKLAMAVE İMHA POLİTİKASI**

İÇİNDEKİLER

[1. AMACI 1](#_Toc186110259)

[2. KİŞİSEL VERİLERİN SAKLANDIĞI KAYIT ORTAMLARI 1](#_Toc186110260)

[3. SAKLAMAYI GEREKTİREN SEBEPLERE İLİŞKİN AÇIKLAMALAR 1](#_Toc186110261)

[4. KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN ALINAN TEDBİRLER 2](#_Toc186110262)

[4.1 Teknik Tedbirler 2](#_Toc186110263)

[4.2 İdari Tedbirler 3](#_Toc186110264)

[5. KİŞİSEL VERİLERİN İMHA EDİLMESİNE İLİŞKİN ALINAN TEDBİRLER 4](#_Toc186110265)

[5.1 Kişisel Verilerin Silinmesi, Yok Edilmesi ve Anonim Hale Getirilmesine İlişkinYöntemler 5](#_Toc186110266)

[5.1.1 Kişisel VerilerinSilinmesi 5](#_Toc186110267)

[5.1.2 Kişisel Verilerin YokEdilmesi 5](#_Toc186110268)

[5.1.3 Kişisel Verileri Anonim Hale Getirilmesi 5](#_Toc186110269)

[6. KİŞİSEL VERİLERİ SAKLAMA VE İMHA SÜRELERİ 6](#_Toc186110270)

[7. PERİYODİK İMHA SÜRELERİ 7](#_Toc186110271)

[8. PERSONEL 7](#_Toc186110272)

[9. RİSK YÖNETİMİ VE DEĞERLENDİRME PROSEDÜRLERİ 7](#_Toc186110273)

[10. REVİZYON VE YÜRÜRLÜKTEN KALDIRMA 7](#_Toc186110274)

[11. YÜRÜRLÜK 8](#_Toc186110275)

[EK1- Veri Saklama ve İmha Süreleri 9](#_Toc186110276)

[EK 2-Kişisel VeriSaklama, İmha ileGörevli Personel Tablosu 11](#_Toc186110277)

## AMACI

SERHAT KAFTAN **(“Nero Pin”)** ait işbu Kişisel Veri Saklama ve İmha Politikası **(“Saklama ve İmha Politikası”)** ile kişisel verilerin 6698 sayılı Kişisel Verilerin Korunması Kanununa **(“Kanun”)** uygun olarak teknik ve idari korunması, kişisel verilerin işlenme şartlarının ortadan kalkması halinde, 28/10/2017 tarihli Resmi Gazete’de yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik **(“Yönetmelik”)** hükümlerinin uygulamasını düzenlemek amacıyla çıkarılmaktadır.

Bu politika, kişisel verilerin hukuka uygun olarak işlenmesi ve imhasına yönelik süreçlerin etkin bir şekilde yönetilmesi amacıyla, gerektiğinde güncellenmek üzere düzenlenmiştir. Politikanın son güncel hali www.neropin.com üzerinden erişilebilir olacaktır.

## KİŞİSEL VERİLERİN SAKLANDIĞI KAYIT ORTAMLARI

Veri sahiplerine ait kişisel veriler, **Nero Pin** tarafından aşağıdaki listelenen ortamlarda başta Kanun hükümleri olmak üzere ilgili mevzuata uygun olarak güvenli bir şekilde saklanmaktadır:

**Elektronik ortamlar:**

* + CRM
  + MS SQLServer
  + E-PostaKutusu
  + Microsoft OfficeProgramları
  + Görüntü Kayıt Cihazları

**Fiziksel ortamlar:**

* + Birim Dolapları
  + Klasörler
  + Arşiv

## SAKLAMAYI GEREKTİREN SEBEPLERE İLİŞKİN AÇIKLAMALAR

**Veri sahiplerine ait kişisel veriler, Nero Pin tarafından özellikle:**

1. Faaliyetlerin sürdürülebilmesi,
2. Hukuki yükümlülüklerin yerine getirilebilmesi,
3. Çalışan haklarının ve yan haklarının planlanması ve ifası,
4. İş ilişkilerinin yönetilebilmesi,

Amacıyla yukarıda sayılan fiziki veyahut elektronik ortamlarda güvenli bir biçimde Kanun ve diğer ilgili mevzuatta belirtilen sınırlar çerçevesinde saklanmaktadır.

**Saklamayı gerektiren sebepler:**

1. Kişisel verilerin sözleşmelerin kurulması ve ifası ile doğrudan doğruya ilgili olması,
2. Kişisel verilerin bir hakkın tesisi, kullanılması veya korunması,
3. Kişisel verilerin kişilerin temel hak ve özgürlüklerine zarar vermemek kaydıyla, **Nero Pin**’ in meşru menfaatinin olması,
4. Kişisel verilerin **Nero Pin**’ in herhangi bir hukuki yükümlülüğünü yerine getirmesi,
5. Mevzuatta kişisel verilerin saklanmasının açıkça öngörülmesi,
6. Veri sahiplerinin açık rızasının alınmasını gerektiren saklama faaliyetleri açısından veri sahiplerinin açık rızasının bulunması.

Yönetmelik uyarınca, aşağıda sayılan hallerde veri sahiplerine ait kişisel veriler, **Nero Pin** tarafından re’ sen yahut talep üzerine silinir, yok edilir veya anonim hale getirilir:

1. Kişisel verilerin işlenmesine veya saklanmasına esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya ilgası,
2. Kişisel verilerin işlenmesini veya saklanmasını gerektiren amacın ortadan kalkması,
3. Kanun’un 5. ve 6. maddelerindeki kişisel verilerin işlenmesini gerektiren şartların ortadan kalkması.
4. Kişisel verileri işlemenin sadece açık rıza şartına istinaden gerçekleştiği hallerde, ilgili kişinin rızasını geri alması,
5. İlgili kişinin, Kanun’un 11. Maddesinin 2 (e) ve (f) bentlerindeki hakları çerçevesinde kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin yaptığı başvurunun veri sorumlusu tarafından kabul edilmesi,
6. Veri sorumlusunun, ilgili kişi tarafından kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesi talebi ile kendisine yapılan başvuruyu reddetmesi, verdiği cevabın yetersiz bulunması veya Kanun’da öngörülen süre içinde cevap vermemesi hallerinde; Kurul’a şikâyette bulunulması ve bu talebin Kurul tarafından uygun bulunması,
7. Kişiselverilerinsaklanmasınıgerektirenazamisüreningeçmişolmasına rağmen, kişisel verileri daha uzun süre saklamayı haklı kılacak herhangi bir şartın mevcutolmaması.

## KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN ALINAN TEDBİRLER

**Nero Pin**, Kanun’un 12. maddesine uygun olarak, işlemekte olduğu kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, verilere hukuka aykırı olarak erişilmesini önlemek ve verilerin muhafazasını sağlamak için uygun güvenlik düzeyini sağlamaya yönelik gerekli teknik ve idari tedbirleri almakta, bu kapsamda gerekli denetimleri yapmak veya yaptırmaktadır. İşlenen kişisel verilerin teknik ve idari tüm tedbirler alınmış olmasına rağmen, kanuni olmayan yollarla üçüncü kişiler tarafından ele geçirilmesi durumunda, **Nero Pin** bu durumu mümkün olan en kısa süre içerisinde ilgili birimlere haber verir.

## 4.1 Teknik Tedbirler

* + Ağ güvenliği ve uygulama güvenliği sağlanmaktadır.
  + Ağ yoluyla kişisel veri aktarımlarında kapalı sistem ağ kullanılmaktadır.
  + Anahtar yönetimi uygulanmaktadır.
  + Bilgi teknolojileri sistemleri tedarik, geliştirme ve bakımı kapsamındaki güvenlik önlemleri alınmaktadır.
  + Çalışanlar için veri güvenliği konusunda belli aralıklarla eğitim ve farkındalık çalışmaları yapılmaktadır.
  + Çalışanlar için yetki matrisi oluşturulmuştur.
  + Erişim, bilgi güvenliği, kullanım, saklama ve imha konularında kurumsal politikalar hazırlanmış ve uygulamaya başlanmıştır.
  + Gizlilik taahhütnameleri yapılmaktadır.
  + Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkileri kaldırılmaktadır.
  + Güncel anti-virüs sistemleri kullanılmaktadır.
  + Güvenlik duvarları kullanılmaktadır.
  + Güvenlik duvarları ve saldırı önleme sistemleri düzenli olarak güncellenir.
  + DDoS saldırılarına karşı altyapısal koruma sağlanır.
  + Hassas veriler üzerinde yapılan tüm işlemler, log kayıtlarına alınır ve denetlenir.
  + İmzalanan sözleşmeler veri güvenliği hükümleri içermektedir.
  + Kişisel veri güvenliği politika ve prosedürleri belirlenmiştir.
  + Kişisel veri güvenliği sorunları hızlı bir şekilde raporlanmaktadır.
  + Kişisel veri güvenliğinin takibi yapılmaktadır.
  + Kişisel veri içeren fiziksel ortamlara giriş çıkışlarla ilgili gerekli güvenlik önlemleri alınmaktadır.
  + Kişisel veri içeren fiziksel ortamların dış risklere (yangın, sel vb.) karşı güvenliği sağlanmaktadır.
  + Kişisel veri içeren ortamların güvenliği sağlanmaktadır.
  + Kişisel veriler mümkün olduğunca azaltılmaktadır.
  + Kişisel veriler yedeklenmekte ve yedeklenen kişisel verilerin güvenliği de sağlanmaktadır.
  + Kullanıcı hesap yönetimi ve yetki kontrol sistemi uygulanmakta olup bunların takibi de yapılmaktadır.
  + Kurum içi periyodik ve/veya rastgele denetimler yapılmakta ve yaptırılmaktadır.
  + Log kayıtları kullanıcı müdahalesi olmayacak şekilde tutulmaktadır.
  + Mevcut risk ve tehditler belirlenmiştir.
  + Özel nitelikli kişisel veri güvenliğine yönelik protokol ve prosedürler belirlenmiş ve uygulanmaktadır.
  + Saldırı tespit ve önleme sistemleri kullanılmaktadır.
  + Şifreleme yapılmaktadır.
  + Taşınabilir bellek, CD, DVD ortamında aktarılan özel nitelikli kişiler veriler şifrelenerek aktarılmaktadır.
  + Veri işleyen hizmet sağlayıcılarının veri güvenliği konusunda belli aralıklarla denetimi sağlanmaktadır.
  + Veri işleyen hizmet sağlayıcılarının, veri güvenliği konusunda farkındalığı sağlanmaktadır.
  + Veri tabanları üzerinde düzenli olarak güvenlik denetimleri gerçekleştirilir ve log kayıtları yalnızca yetkili kişiler tarafından erişilebilir hale getirilir.
  + Kritik veri erişimleri şifreleme yöntemleri ile koruma altına alınmaktadır.
  + Nero Pin, siber güvenlik olaylarına karşı önleyici ve düzeltici tedbirler alır. Herhangi bir saldırı veya güvenlik ihlali durumunda, olayın boyutu analiz edilir ve anında müdahale edilir. Bu süreçler aşağıdaki adımları içerir:
    - Olay tespiti ve önceliklendirme,
    - Etkilenen sistemlerin ve verilerin tespiti,
    - İlgili tarafların bilgilendirilmesi,
    - Verilerin kurtarılması ve sistemlerin yeniden yapılandırılması.

## 4.2 İdari Tedbirler

* + Çalışanlar, kişisel verilere hukuka aykırı erişimi engellemek için alınacak teknik tedbirler konusunda eğitilmektedir.
  + İş birimi bazında kişisel veri işlenmesi hukuksal uyum gerekliliklerine uygun olarak **Nero Pin** içinde kişisel verilere erişim ve yetkilendirme süreçleri tasarlanmakta ve uygulanmaktadır. Erişimin sınırlandırılmasında verinin özel nitelikli olup olmadığı ve önem derecesi de dikkate alınır.
  + **Nero Pin** personeli ile arasındaki ilişkiyi düzenleyen ve kişisel veri içeren her türlü belgeye kişisel verilerin hukuka uygun olarak işlenmesi için Kanun ile öngörülen yükümlülüklere uygun hareket edilmesi gerektiği, kişisel verilerin ifşa edilmemesi gerektiği, kişisel verilerin hukuka aykırı olarak kullanılmaması gerektiği ve kişisel verilere ilişkin gizlilik yükümlülüğünün **Nero Pin** ile olan iş akdinin sona ermesinden sonra dahi devam ettiği yönünde kayıtlar eklemiştir.
  + Çalışanlar, öğrendikleri kişisel verileri Kanun hükümlerine aykırı olarak başkasına açıklayamayacağı ve işleme amacı dışında kullanamayacağı ve bu yükümlülüğün görevden ayrılmalarından sonra da devam edeceği konusunda bilgilendirilmekte ve bu doğrultuda kendilerinden gerekli taahhütler alınmaktadır.
  + **Nero Pin** tarafından kişisel verilerin hukuka uygun olarak aktarıldığı kişiler ile akdedilen sözleşmelere; kişisel verilerin aktarıldığı kişilerin, kişisel verilerin korunması amacıyla gerekli güvenlik tedbirlerini alacağına ve kendi kuruluşlarında bu tedbirlere uyulmasını sağlayacağına ilişkin hükümler eklenmektedir.
  + İşlenen kişisel verilerin hukuka aykırı yollarla başkaları tarafından elde edilmesi hâlinde, bu durumu en kısa sürede ilgilisine ve Kurul’a bildirir.
  + Gerekli hallerde kişisel verilerin işlenmesi hakkında bilgili ve deneyimli personel istihdam eder ve personeline kişisel verilerin korunması mevzuatı ve veri güvenliği kapsamında eğitimleri verir.
  + **Nero Pin**, Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapar ve yaptırır. Denetimler sonucunda ortaya çıkan gizlilik ve güvenlik zafiyetlerini giderir.
  + Kişisel verilerin işlenmesi ve güvenliği konularında düzenli olarak personel eğitimleri düzenlenir. Bu eğitimler, çalışanların ilgili mevzuata uyum sağlama kapasitelerini artırmayı hedefler.
  + Şirket içi denetim mekanizmaları periyodik olarak devreye alınır; bu denetimler sırasında gizlilik sözleşmelerine ve politikalara uyum kontrol edilir.
  + **Nero Pin**, işlenen kişisel verilerin, işleme amacı için gerekli olan minimum seviyede tutulmasını sağlamak için süreçlerini sürekli gözden geçirir. Gereksiz veri işlememeye ve saklamamaya yönelik önlemler alınır.

## KİŞİSEL VERİLERİN İMHA EDİLMESİNE İLİŞKİN ALINAN TEDBİRLER

**Nero Pin** ilgili kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kendi kararına istinaden veya kişisel veri sahibinin talebi üzerine kişisel verileri silebilir veya yok edebilir. Kişisel verilerin silinmesi akabinde ilgili kişiler hiçbir şekilde silinen verilere tekrardan erişilemeyecek ve kullanılmayacaktır. **Nero Pin** tarafından kişisel verilerin imha süreçlerinin tanımlanması ve takip edilmesine ilişkin etkin bir veri takip süreci yönetilecektir. Yürütülen süreç sırası ile silinecek verilerin tespit edilmesi, ilgili kişilerin tespiti, kişilerin erişim yöntemlerinin tespiti ve hemen akabinde verilerin silinmesi olacaktır.

**Nero Pin** kişisel verileri yok etmek, silmek veya anonim hale getirmek için verilerin kaydedildiği ortama bağlı olarak aşağıda belirtilen yöntemlerin bir veya birkaçını kullanabilir:

## Kişisel Verilerin Silinmesi, Yok Edilmesi ve Anonim Hale Getirilmesine İlişkinYöntemler

* + 1. **Kişisel VerilerinSilinmesi**

Kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. Kişisel verilerin silinmesi yöntemi olarak **Nero Pin** aşağıdaki yöntemlerden bir veya birkaçını kullanabilir:

* Kağıt ortamında bulunan kişisel veriler karartma yöntemi ile çizilerek, boyanarak, kesilerek veya silinerek işlem uygulanacaktır.
* Fiziksel ortamda saklanan verilerin imha süreçleri sırasında çevresel etkiler göz önünde bulundurulur. Kâğıt imha süreçleri geri dönüşüm ilkelerine uygun şekilde gerçekleştirilir.
* Merkezi dosyada yer alan ofis dosyaları için kullanıcı(lar)nın erişim hakkı(ları) ortadan kaldırılacaktır.
* Veri tabanlarında bulunan kişisel bilgilerin bulunduğu satırlar yahut sütunlar ‘Delete’ komutu ile silinecektir.
* Fiziksel ortamda saklanan evraklar, imha işlemleri sırasında geri dönüştürülmeyecek şekilde parçalanır.
* Elektronik ortamdaki dosyalar, verinin hiçbir şekilde geri getirilememesi için uluslararası standartlara uygun şekilde yok edilir.

Gerekli olduğu zaman bir uzman tarafından yardım alınarak güvenli olarak silinecektir.

## Kişisel Verilerin YokEdilmesi

Kişisel verilerin yok edilmesi, kişisel verilerin aşağıdaki yöntemlerle hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir.

Fiziksel Yok Etme

Kâğıt İmha Makinesi ile YokEtme

De-manyetize Etme: Manyetik medyanın yüksek manyetik alanlara maruz kalacağı özel cihazlardan geçirilerek üzerindeki verilerin okunamaz bir biçimde bozulması yöntemidir.

## Kişisel Verileri Anonim Hale Getirilmesi

Kişisel verilerin anonim hale getirilmesi, kişisel verilerin başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesini ifade eder. **Nero Pin** kişisel verileri anonim hale getirmek için aşağıda belirtilen yöntemlerin bir veya birkaçını kullanabilir:

**Maskeleme (Masking):**Veri maskeleme ile kişisel verinin temel belirleyici bilgisini veri seti içerisinden çıkartılarak kişisel verinin anonim hale getirilmesi yöntemidir.

**Kayıtları Çıkartma:** Kayıttan çıkarma yönteminde veriler arasında tekillik ihtiva eden veri satırı kayıtlar arasından çıkarılarak saklanan veriler anonim hale getirilmektedir.

**Bölgesel Gizleme:** Bölgesel gizleme yönteminde ise tek bir verinin çok az görülebilir bir kombinasyon yaratması sebebi ile belirleyici niteliği mevcut ise ilgili verinin gizlenmesi anonimleştirmeyi sağlamaktadır.

**Global Kodlama:** Veri türetme yöntemi ile kişisel verinin içeriğinden daha genel bir içerik oluşturulmakta ve kişisel verinin herhangi bir kişiyle ilişkilendirilemeyecek hale getirilmesi sağlanmaktadır. Örneğin; doğum tarihleri yerine yaşların belirtilmesi, açık adres yerine ikamet edilen bölgenin belirtilmesi.

**Gürültü Ekleme:** Verilere gürültü ekleme yöntemi özellikle sayısal verilerin ağırlıklı olduğu bir veri setinde mevcut verilere belirlenen oranda artı veya eksi yönde birtakım sapmalar eklenerek veriler anonim hale getirilmektedir. Örneğin, kilo değerlerinin olduğu bir veri grubunda (+/-) 3 kg sapması kullanılarak gerçek değerlerin görüntülenmesi engellenmiş ve veriler anonimleştirilmiş olur. Sapma her değere eşit ölçüde uygulanır.

Kanun’un 28. maddesine uygun olarak; anonim hale getirilmiş olan kişisel veriler araştırma, planlama ve istatistik gibi amaçlarla işlenebilir. Bu tür işlemeler Kanun kapsamı dışında olup, kişisel veri sahibinin açık rızası aranmayacaktır.

**Nero Pin** kişisel verinin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin re’ sen karar alabilecek ve seçmiş olduğu kategoriye göre kullanacağı yöntemi de serbestçe belirleyebilecektir. Ayrıca Yönetmelik’in 13. maddesi kapsamında ilgili kişinin başvuru esnasında kendisine ait kişisel verinin silinmesi, yok edilmesi yahut anonim hale getirilmesi kategorilerinden birini seçmesi halinde de ilgili kategoride kullanılacak yöntemler konusunda **Nero Pin** serbesti içinde olacaktır.

## KİŞİSEL VERİLERİ SAKLAMA VE İMHA SÜRELERİ

**Nero Pin**, kişisel verileri işlendikleri amaç için Ek-1’de belirtilen süreler boyunca saklar. Mevzuatta söz konusu kişisel verinin saklanmasına ilişkin olarak bir süre öngörülmüş ise bu süreye riayet edilir. Mevzuatta öngörülmüş bir süre olmaması halinde kişisel veriler Ek-1’deki tabloda yer alan kişisel verilerin tutulması için azami süre boyunca saklanacaktır. Bu süreler; **Nero Pin**’ in veri kategorileri ve veri sahibi kişi grupları değerlendirilerek; bu değerlendirme sonucu elde edilen verilerin kanunlarda yer alan yükümlülüklerin yerine getirilmesini sağlayacak ve azami Türk Borçlar Kanunu’nda yer alan zamanaşımı süresi (10 yıl) gözetilerek belirlenmiştir.

Bu sürelerin sona ermesi dolayısıyla silme, yok etme veya anonim hale getirme yükümlülüğünün ortaya çıktığı durumda **Nero Pin** bu tarihi takip eden ilk periyodik imha işleminde kişisel verileri siler, yok eder veya anonim hale getirir.

Kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesiyle ilgili yapılan bütün işlemler kayıt altına alınır ve söz konusu kayıtlar, diğer hukuki yükümlülükler hariç olmak üzere en az üç yıl süreyle saklanır.

## PERİYODİK İMHA SÜRELERİ

Yönetmeliğin 11’inci maddesi gereğince, periyodik imha süresini 6 ay olarak belirlenmiştir. Buna göre, her yıl haziran ve aralık aylarında periyodik imha işlemi gerçekleştirilir. Söz konusu sistemlerde bilgilerin tekrar geri getirilmeyecek şekilde, verilerin kaydedildiği varsa evrak, dosya, CD, disket, hard disk gibi araçlardan geri dönüştürülmeyecek şekilde silinecektir.

Periyodik imha işlemleri için özel bir ekip atanır ve bu ekip, imha süreçlerinin mevzuata uygun şekilde gerçekleştirilmesini sağlar. Periyodik imha işlemlerine ilişkin tüm kayıtlar, daha sonraki denetimler için güvenli bir şekilde saklanır.

## PERSONEL

Kanun kapsamında **Nero Pin** veri sorumlusu sıfatıyla, Yönetmelik’in 11. maddesinin 1. fıkrasına dayanarak, Kanunun veri saklama ve imha süreci uygulanması bakımından yükümlülükleri yerine getirilecek personelin unvanları, birimleri ve görev tanımları Saklama ve İmha Politikası Ek-2’de yer alan tablo ile belirlenmiştir.

Sınırları belirlenmiş bu kişiler Türk Ticaret Kanunu, Borçlar Kanunu ve Türk Ceza Kanunu kapsamında kendi yetki sınırları içinde gerçekleşen işlem ve eylemlerden sorumludur. Özellikle Kollukta, Savcılıklarda, kamu kurumlarında ve mahkemelerde **Nero Pin’** i temsil etme ile ifade vermeye yetkili olarak **Nero Pin** Kişisel Verileri Koruma Komitesi Başkanı seçilmiştir. Her bir departman sorumlusu, departmanlardaki ilgili kullanıcıların Kanun ve Yönetmelik çerçevesinde hazırlanan Saklama ve İmha Politikası ve Kişisel Veri Politikası’na uygun davranıp davranmadığını denetlemekle yükümlü olacaktır. Tüm departman sorumluları belirtilen periyodik imha sürelerinde işbu Saklama ve İmha Politikası doğrultusunda gerçekleştirdiği işlemleri **Nero Pin** Kişisel Verileri Koruma Komitesi Başkanı’na raporlayacaktır. Bu raporlar için yapılan çalışma sonuçlarında çıkan karar uygulamaya konulacaktır.

## RİSK YÖNETİMİ VE DEĞERLENDİRME PROSEDÜRLERİ

Nero Pin, kişisel verilerin korunmasına yönelik potansiyel riskleri belirlemek ve bu risklere karşı proaktif önlemler almak amacıyla düzenli risk değerlendirme çalışmaları yapar. Bu kapsamda:

* Mevcut güvenlik açıkları ve tehditler analiz edilir.
* Risk seviyesine göre aksiyon planları hazırlanır.
* Risk değerlendirme sonuçları yılda en az bir kez gözden geçirilir ve gerektiğinde revize edilir.

## REVİZYON VE YÜRÜRLÜKTEN KALDIRMA

Saklama ve İmha Politikasının değiştirilmesi, yürürlükten kaldırılması halinde yeni düzenleme [www.neropin.com](http://www.neropin.com) sitesinden ilan edilecektir.

Politika üzerinde yapılan her türlü değişiklik, değişiklik tarihleriyle birlikte kayıt altına alınır. Yeni versiyonlar, tüm personel ve ilgili taraflara duyurulur.

Veri sahipleri, kişisel verilerine erişim, düzeltme, silme ve işleme faaliyetlerine dair bilgilendirme taleplerini **Nero Pin**'in resmi iletişim kanalları üzerinden iletebilir. Talepler yasal süreler içinde sonuçlandırılır ve başvuru sonuçları yazılı olarak bildirilir.

## YÜRÜRLÜK

Bu Saklama ve İmha Politikası yayınlandığı tarihinde yürürlüğe girer.

**EKLER**

**EK 1-Veri Saklama ve İmha Süreleri**

**EK 2-Kişisel Veri Saklama, İmha ile Görevli Personel Tablosu**

**EK1- Veri Saklama ve İmha Süreleri**

|  |  |  |
| --- | --- | --- |
| **Veri Kategorisi** | **Saklama Süresi** | **İmha Süresi** |
| Kimlik | İşlem tarihi veya hukuki ilişkinin sonlanmasından itibaren 10 yıl | Saklama süresinin bitimini takip eden ilk periyodik imha süresinde |
| İletişim | İşlem tarihi veya hukuki ilişkinin sonlanmasından itibaren 10 yıl | Saklama süresinin bitimini takip eden ilk periyodik imha süresinde |
| Lokasyon | İşlem tarihi veya hukuki ilişkinin sonlanmasından itibaren 10 yıl | Saklama süresinin bitimini takip eden ilk periyodik imha süresinde |
| Özlük | İstihdamın sonlanmasından itibaren 10 yıl | Saklama süresinin bitimini takip eden ilk periyodik imha süresinde |
| Hukuki İşlem | Yargı kararının kesinleşmesinden itibaren 5 yıl | Saklama süresinin bitimini takip eden ilk periyodik imha süresinde |
| İşlem tarihi veya hukuki ilişkinin sonlanmasından itibaren 10 yıl | Saklama süresinin bitimini takip eden ilk periyodik imha süresinde |
| Müşteri İşlem | İşlem tarihi veya hukuki ilişkinin sonlanmasından itibaren 10 yıl | Saklama süresinin bitimini takip eden ilk periyodik imha süresinde |
| Fiziksel Mekân Güvenliği | 30 gün | Saklama süresinin bitimini takip eden ilk periyodik imha süresinde |
| İşlem Güvenliği | İşlem tarihi veya hukuki ilişkinin sonlanmasından itibaren 10 yıl | Saklama süresinin bitimini takip eden ilk periyodik imha süresinde |
| Risk Yönetimi | İşlem tarihi veya hukuki ilişkinin sonlanmasından itibaren 10 yıl | Saklama süresinin bitimini takip eden ilk periyodik imha süresinde |
| Finans | İşlem tarihi veya hukuki ilişkinin sonlanmasından itibaren 10 yıl | Saklama süresinin bitimini takip eden ilk periyodik imha süresinde |
| Mesleki Deneyim | İstihdamın sonlanmasından itibaren 10 yıl | Saklama süresinin bitimini takip eden ilk periyodik imha süresinde |
| Pazarlama | İstihdamın sonlanmasından itibaren 10 yıl | Saklama süresinin bitimini takip eden ilk periyodik imha süresinde |
| Görsel ve İşitsel Kayıtlar | İşlem tarihi veya hukuki ilişkinin sonlanmasından itibaren 10 yıl | Saklama süresinin bitimini takip eden ilk periyodik imha süresinde |
| Sendika Üyeliği | İstihdamın sonlanmasından itibaren 10 yıl | Saklama süresinin bitimini takip eden ilk periyodik imha süresinde |
| Sağlık Bilgileri | 15 yıl | Saklama süresinin bitimini takip eden ilk periyodik imha süresinde |
| Ceza Mahkûmiyeti ve Güvenlik Tedbirleri | İstihdamın sonlanmasından itibaren 10 yıl | Saklama süresinin bitimini takip eden ilk periyodik imha süresinde |
| Aile Bilgileri | 10 Yıl | Saklama süresinin bitimini takip eden ilk periyodik imha süresinde |
| Çalışma Verisi | 10 Yıl | Saklama süresinin bitimini takip eden ilk periyodik imha süresinde |
| Web Sitesi Kullanım Verileri | 2 Yıl | Saklama süresinin bitimini takip eden ilk periyodik imha süresinde |
| Talep/Şikâyet Yönetimi Bilgisi | 2 Yıl | Saklama süresinin bitimini takip eden ilk periyodik imha süresinde |
| İtibar Yönetimi Bilgisi | 10 Yıl | Saklama süresinin bitimini takip eden ilk periyodik imha süresinde |
| Olay Yönetimi Bilgisi | 2 Yıl | Saklama süresinin bitimini takip eden ilk periyodik imha süresinde |
| İmzalar | 10 Yıl | Saklama süresinin bitimini takip eden ilk periyodik imha süresinde |
| Sigorta Bilgileri | İstihdamın sonlanmasından itibaren 10 yıl | Saklama süresinin bitimini takip eden ilk periyodik imha süresinde |
| Araç Bilgileri | 10 Yıl | Saklama süresinin bitimini takip eden ilk periyodik imha süresinde |
| Uyum Bilgileri | 10 Yıl | Saklama süresinin bitimini takip eden ilk periyodik imha süresinde |
| Denetim ve Teftiş | 10 Yıl | Saklama süresinin bitimini takip eden ilk periyodik imha süresinde |
| Yabancı Oturma İzni Bilgileri | İstihdamın sonlanmasından itibaren 10 yıl | Saklama süresinin bitimini takip eden ilk periyodik imha süresinde |

**EK 2-Kişisel VeriSaklama, İmha ileGörevli Personel Tablosu**

|  |  |  |
| --- | --- | --- |
| **Personel** | **Görev** | **Sorumluluk** |
| Personel Sorumlusu | Uygulama sorumlusu | Görevi içindeki süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecininyönetimi |
| İdari Mali İşler Sorumlusu | Uygulama sorumlusu | Görevi içindeki süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecininyönetimi |
|  | Uygulama sorumlusu | Görevi içindeki süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecininyönetimi |